University of Washington School of Dentistry
Office of Regional Affairs
Salesforce.com Records Scanning Policy

Purpose

Retention of Records

The purpose of this document is to establish a consistent process that enables the Office of Regional Affairs and RIDE (ORA/RIDE) to replace paper records with scanned, electronic records while ensuring adherence to retention requirements. This process is based upon UW guidance and on Chapter 434-663 of the Washington Administrative Code (WAC).

All records have a specific amount of time they must be maintained, called a "retention period," that is based on the content of a record. Retention periods are found on the University General Records Retention Schedule. Retention periods included in the Records Retention Schedule apply to all records regardless of their physical form or characteristics.

Once ORA/RIDE paper records are scanned according to the technical requirements outlined in this document, the paper records can be destroyed. It is, however, important to note that the retention period which would have been applied to the paper record must instead be applied to the scanned record. The retention period also applies to records originating and remaining in electronic form.

Technical Scanning Instructions

Formats and Scanning Densities

Black and white, gray, and color paper records can be scanned. Any kind of record can be scanned including color text documents, photographs, maps, plans, diagrams, and drawings.

- Scanners must be set at a minimum of 300 dpi (dots per inch): and
- Scanned records must be saved as searchable PDF files.

Quality Control

Scanned document images must be inspected visually to ensure they are complete (the entire document has been captured), clear and easily read. It is required that:

- At least every 10th page of each document is reviewed to ensure the scanning quality is consistent and the images are usable. If and when visual inspection raises doubts, the scanned records should be compared to the original paper document to ensure accuracy; and
- The number of original paper pages in a document is compared to the number of pages in the scanned record to ensure that every page of the document was scanned.

Image Enhancement

Problems with a scanned image can make it difficult to read and less than usable. If the scanned document is to replace the original paper record the following common problems must be corrected as noted.

- Speckles or spots on the scanned image that obscure its contents:
  - Clean the glass on the scanner and rescan the paper.
- Skewed images that are not properly aligned:
  - Rescan the paper so that the image appears straight.
- All portrait orientation pages should be rotated to read from left to right; all landscape orientation pages should be rotated with the top of the page facing the left.
- Sometimes only part of the document is captured by the scanner:
  - Rescan the paper so that it is properly aligned and the entire page is included in the scanned image.
- If the scanned record is of poor quality and is not clearly readable:
  - Reset the dpi (dots per inch) setting on the scanner to a setting higher than 300 dpi and scan again. Keep increasing the dpi until the record is as readable as possible.

Poor Quality Images

Sometimes the condition of the original paper record precludes a good quality scanned image from being produced. In these cases ORA/RIDE will document the problem to avoid future confusion over the poor quality of the scanned image, and retain the paper copy.

- The person scanning will confer with the ORA/RIDE authorized records monitor to make the determination of whether a scan is of usable quality.
- If the best scan is deemed unusable, tag the image with "best scan possible – paper retained", using Acrobat Pro "Additional Metadata" in the Document Properties description tab.
- Keep the paper copy of the record in a location determined by the authorized records monitor.
- The scanned copy will still be electronically added to the appropriate account in the Salesforce database.

Managing Scanned Records

File Naming Convention

Scanned records will be named following a convention appropriate to the type of record. These conventions are noted in the Salesforce Naming Conventions document located on SharePoint.

Organizing and Filing Scanned Records

All scanned records will be uploaded as an attachment to the appropriate record in the Salesforce database. Scanned records should not be saved to thumb drives, the shared drive (P-drive), or to the hard drive on a personal computer.

The agreement renewal date and date of termination will be documented in a task connected to the Salesforce account. The task will include a due date for action so that records can be readily accessed and managed for renewal or destruction at the end of their retention period.

Modifying Scanned Records

It is important to ensure that the original content of a scanned record is not altered or modified once it has been finalized. Scanned records will be "read only" PDF format, to ensure that there is no improper alteration or modification. However, many times it is useful to add a note on a PDF using a text box or other Adobe annotation tool. This is not considered a modification of the scanned record and is an acceptable and practical way to make notes on an electronic record. Notes can also be added to the description box on the account in the Salesforce database.

Destruction of Scanned Records

All scanned documents must be kept through the duration of their retention period. The deletion approval process at ORA/RIDE includes:

- Approver: Typically the unit head or office supervisor. Responsible for authorizing the deletion of records at the end of the retention period.
- Authorized records monitor: Responsible for monitoring records retention and identifying records due for deletion and, upon approval, deleting the records.
- Only authorized individuals (positions) may delete files. Ability to delete files from the database or networked storage location will be restricted to authorized users only.
- NOTE: All records pertaining to ongoing or pending audits, lawsuits (or even reasonably anticipated lawsuits), or public disclosure proceedings must not be destroyed, damaged or altered until the issue is resolved. The Approver is responsible for monitoring which if any records are subject to such restrictions. Once the issue is resolved, the Approver must be informed that records may be destroyed before giving approval for records destruction.

Once a due date reminder appears on the homepage of Salesforce, the authorized records monitor will review the account and verify that the file has reached the end of its retention period. This individual will send the name of the document and the name of the related account to the ORA/RIDE's Approver for destruction approval. Once the Approver returns the email with their approval, the authorized records monitor will delete the file and record the destroyed file on the Records Destruction Log. The log will include: document type, termination date, date deleted, deleted by, and deletion authorized by. The authorized records monitor will then make a note in the description box of the account indicating that the file has been destroyed.

Migration and Preservation Strategies

ORA/RIDE currently does not maintain any archival records or records with a retention period of more than 6 years that would require a migration and preservation strategy before the original paper documents can be destroyed. If this changes, a migration and preservation strategy will be added to this policy.

Security Standards

Salesforce.com utilizes some of the most advanced technology for Internet security available today. When the site is accessed using a supported web browser, Secure Socket Layer (SSL) technology protects information using both server authentication and data encryption.

Salesforce.com provides each user with a unique username and password that must be entered each time a user logs in. Salesforce.com issues a session "cookie" only to record encrypted authentication information for the duration of a specific session. The session "cookie" does not include either the username or password of the user. Salesforce.com does not use "cookies" to store other confidential user and session information, but instead implements more advanced security methods based on dynamic data and encoded session IDs.

Salesforce.com is hosted in a secure server environment (located off-campus) that uses a firewall and other advanced technology to prevent interference or access from outside intruders. All customer data is backed up on tape on a nightly basis, up to the last committed transaction. Salesforce.com further enhances reliability measures by storing all customer data on mirrored disks that are mirrored across different storage cabinets and controllers.

When an employee separates, their immediate manager is responsible for notifying all system owners and operators, or the designated system administrator handling the computer or communications accounts, to close all related accounts and remove all access capabilities related to the separated employee.

Upon receiving notification of termination, Salesforce will close the account on either the requested termination date or upon expiration of the salesforce.com contract. All salesforce.com data will be available for 30 days from the date of termination. The account owner can get an export of all data (including attachments) by using the Data Loader found under Setup – Data Management.

Office machines used to create scans or copies will be checked annually and any copies of records found will be deleted.